UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/614,765	07/07/2003	Paul C. Kocher	24162-08736	8024

26263 7590 06/04/2007

SONNENSCHEIN NATH & ROSENTHAL LLP
P.O. BOX 061080
WACKER DRIVE STATION, SEARS TOWER
CHICAGO, IL 60606-1080

EXAMINER	
POPHAM, JEFFREY D	

ART UNIT	PAPER NUMBER
2137	

MAIL DATE	DELIVERY MODE
06/04/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/614,765	KOCHER ET AL.	
	Examiner	Art Unit	
	Jeffrey D. Popham	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 April 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *2-18* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *2-18* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *07 July 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *See Continuation Sheet*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Continuation of Attachment(s) 3). Information Disclosure Statement(s) (PTO/SB/08), Paper No(s)/Mail Date :20060919, 20060427, 20050606, 20050429, 20041108.

Remarks

Claims 2-18 are pending.

Claim Objections

1. Claims 15 and 16 are objected to because of the following informalities:

   - Claim 15 step (a) recites "said medium uniquely does not uniquely", which should apparently read "said medium does not uniquely".
   - Claim 16, step (e) recites "said optical medium", which appears to be intended to refer to the "digital medium" of the preamble. Clarification is required so that step (e) has antecedent basis.

   Appropriate correction is required.

Information Disclosure Statement

2. The information disclosure statement filed 4/29/2005 fails to comply with 37 CFR 1.98(a)(2), which requires a legible copy of each cited foreign patent document; each non-patent literature publication or that portion which caused it to be listed; and all other information or that portion which caused it to be listed. It has been placed in the application file, but the information referred to therein has not been considered.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 2, 12, and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Asano (U.S. Patent 6,999,587) in view of Benaloh (U.S. Patent 7,065,216).

Regarding Claim 2,

Asano discloses a digital optical medium containing compressed digital audiovisual content with protections against unauthorized copying, comprising:

A digital signature authenticating at least an identifier of the optical medium (Column 7, line 33 to Column 8, line 3);

A digitally-signed list identifying at least one other medium that is revoked (Column 8, lines 10-30);

Digital audiovisual content that is encrypted using broadcast encryption, whereby: each of a plurality of authorized playback devices has cryptographic keys sufficient for decrypting the audiovisual content, and each of a plurality of revoked playback devices do not have keys sufficient for decrypting the audiovisual content (Column 6, lines 29-32; Column 8, lines 45-59; Column 9; lines 35-58; and Column 14, lines 1-63); and

Logic defining an interface usable to control playback of the audiovisual content (Column 6, lines 29-32; and Column 14, lines 1-63);

But does not disclose a plurality of versions of a plurality of portions of the digital audiovisual content where the versions for each portion may be distinguished from each other in pirated recordings of the audiovisual content; the versions are encrypted with different keys, such that each of the authorized playback devices is capable of deciphering at least one, but not all, of the versions for each of the portions; and the combination of the portions decipherable by a given player may be used to identify the player.

Benaloh, however, discloses that the digital audiovisual content is compressed and encrypted, whereby each of a plurality of authorized playback devices has cryptographic keys sufficient for decrypting the audiovisual content, and each of a plurality of unauthorized playback devices do not have keys sufficient for decrypting the audiovisual content (Column 3, line 65 to Column 4, line 6; and Column 9, line 61 to Column 11, line 12); and

A plurality of versions of a plurality of portions of the compressed digital audiovisual content, where: the versions for each portion may be distinguished from each other in pirated recordings of the audiovisual content; the versions are encrypted with different keys, such that each of the authorized playback devices is capable of deciphering at least one, but not all, of the versions for each of the portions; and the combination of the portions decipherable by a given player may be used to identify the player (Column 9, line 61 to Column 11, line 12); and

Logic defining an interface usable to interact with a user and to control playback of the audiovisual content (Figure 1; and Column 3, line 24 to Column 4, line 40). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the digital content protection scheme of Benaloh into the information recording/reproducing system of Asano in order to allow the system to detect pirated copies of content and trace it back to the specific player used to pirate the content while providing all content players with identical data on the storage medium.

Regarding Claim 12,

Asano discloses a device for securely playing digital audiovisual content, the audiovisual content including a plurality of regions each having multiple versions thereof, comprising:

A media drive including a laser for use in reading data from rotating optical media (Column 8, lines 45-58);

A nonvolatile memory containing: a set of cryptographic player keys for use with a broadcast encryption system, and identifiers of revoked media (Column 9; lines 35-58; and Column 11, lines 18-30);

A bulk decryption module for decrypting encrypted audiovisual content from the media (Column 14, lines 1-63); and

Media verification logic configured to verify: whether valid digital signatures contained on the media authenticate the media, and whether

the media are identified as revoked in the nonvolatile memory (Column 9, lines 45-67);

But does not disclose program logic configured to: select a version of each region, and decrypt the selected version, whereby a combination of the versions selected in the course of playing the media uniquely identifies the device; and at least one codec for decompressing the audiovisual content.

Benaloh, however, discloses program logic configured to: select a version of each region, and decrypt the selected version, whereby a combination of the versions selected in the course of playing the media uniquely identifies the device (Column 9, line 61 to Column 11, line 12); and at least one codec for decompressing the audiovisual content (Column 3, line 65 to Column 4, line 6). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the digital content protection scheme of Benaloh into the information recording/reproducing system of Asano in order to allow the system to detect pirated copies of content and trace it back to the specific player used to pirate the content while providing all content players with identical data on the storage medium.

Regarding Claim 15,

Asano as modified by Benaloh discloses the device of claim 12, in addition, Benaloh discloses that the combination of versions selected

during the course of playback of any one medium does not uniquely identify the playback device; and the combination of versions selected during the course of playback of a plurality of the media does uniquely identify the playback device (Column 14, lines 41-50).

4. Claims 3-11, 13, and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Asano in view of Benaloh, further in view of Kyle (U.S. Patent 6,141,681).

Regarding Claim 3,

Asano as modified by Benaloh does not explicitly disclose program logic for an interpreter of a Turing-complete language, where: the program logic is configured to perform a plurality of security checks; and the program logic is configured to permit playback of the audiovisual content provided that the security checks are successful.

Kyle, however, discloses program logic for an interpreter of a Turing-complete language, where: the program logic is configured to perform a plurality of security checks; and the program logic is configured to permit playback of the audiovisual content provided that the security checks are successful (Column 3, line 28 to Column 4, line 30; Column 4, line 57 to Column 5, line 14; and Column 7, line 59 to Column 8, line 5). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the self protecting data package

system of Kyle into the information recording/reproducing system of Asano as modified by Benaloh in order to allow the system to update the player and anti-virus software, thereby maintaining security of the system with ease, as well as to provide self-sufficient data packages that can perform compression, decryption, virus checking, etc. without the need of specialized hardware or software.

Regarding Claim 4,

Asano as modified by Benaloh and Kyle discloses the medium of claim 3, in addition, Kyle discloses that the program logic is configured to invoke at least one cryptographic operation supported by at least one of the authorized playback devices (Column 4, line 57 to Column 5, line 14).

Regarding Claim 5,

Asano as modified by Benaloh and Kyle discloses the medium of claim 3, in addition, Kyle discloses that the program logic is configured to perform at least one operation necessary for decryption of the audiovisual content by at least one authorized playback device (Column 4, line 57 to Column 5, line 14).

Regarding Claim 6,

Asano as modified by Benaloh does not explicitly disclose that a subset of the authorized playback devices encompass a plurality of models, each model having a model-specific vulnerability, and further comprising program logic which, when executed by a device of each

vulnerable model, is configured to: mitigate the vulnerability affecting the vulnerable playback device; and perform at least one operation necessary for the vulnerable playback device to decrypt the audiovisual content.

Kyle, however, discloses that a subset of the authorized playback devices encompass a plurality of models, each model having a model-specific vulnerability, and further comprising program logic which, when executed by a device of each vulnerable model, is configured to: mitigate the vulnerability affecting the vulnerable playback device; and perform at least one operation necessary for the vulnerable playback device to decrypt the audiovisual content (Column 4, lines 34-56; Column 5, lines 32-60; and Column 8, lines 6-19). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the self protecting data package system of Kyle into the information recording/reproducing system of Asano as modified by Benaloh in order to allow the system to update the player and anti-virus software, thereby maintaining security of the system with ease, as well as to provide self-sufficient data packages that can perform compression, decryption, virus checking, etc. without the need of specialized hardware or software.

Regarding Claim 7,

Asano as modified by Benaloh and Kyle discloses the medium of claim 6, in addition, Kyle discloses that the program logic includes

executable code for a Turing-complete virtual machine (Column 3, line 66 to Column 4, line 6; and Column 7, line 59 to Column 8, line 5).

Regarding Claim 8,

Asano as modified by Benaloh and Kyle discloses the medium of claim 6, in addition, discloses that the operation necessary to decrypt includes updating a cryptographic key contained in the playback device (Column 12, lines 35-67).

Regarding Claim 9,

Asano as modified by Benaloh and Kyle discloses the medium of claim 6, in addition, Kyle discloses that the program logic for mitigating includes native executable code configured to detect whether the security of a vulnerable device has been compromised (Column 4, lines 34-56; Column 5, lines 32-60; and Column 8, lines 6-19).

Regarding Claim 10,

Asano as modified by Benaloh and Kyle discloses the medium of claim 6, in addition, Kyle discloses that the program logic for mitigating includes native executable code configured to correct a vulnerability in a vulnerable device (Column 4, lines 34-56; Column 5, lines 32-60; and Column 8, lines 6-19).

Regarding Claim 11,

Asano as modified by Benaloh and Kyle discloses the medium of claim 6, in addition, Benaloh discloses that the player comprises firmware

(Column 7, lines 48-53; and Column 11, lines 13-42); and Kyle discloses that the program logic for mitigating includes an upgrade to the player for correcting at least one vulnerability (Column 3, line 28 to Column 4, line 30; Column 4, line 57 to Column 5, line 14; and Column 7, line 59 to Column 8, line 19).

Regarding Claim 13,

Asano as modified by Benaloh does not explicitly disclose an interpreter for a Turing-complete language, where the interpreter is configured to obtain program logic from the drive and execute the program logic.

Kyle, however, discloses an interpreter for a Turing-complete language, where the interpreter is configured to obtain program logic from the drive and execute the program logic (Column 3, line 28 to Column 4, line 30; Column 4, line 57 to Column 5, line 14; and Column 7, line 59 to Column 8, line 5). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the self protecting data package system of Kyle into the information recording/reproducing system of Asano as modified by Benaloh in order to allow the system to update the player and anti-virus software, thereby maintaining security of the system with ease, as well as to provide self-sufficient data packages that can perform compression, decryption, virus checking, etc. without the need of specialized hardware or software.

Regarding Claim 16,

Asano discloses a method for playing encrypted digital audiovisual content from a digital medium, comprising:

Verifying a digital signature authenticating the medium (Column 9, lines 45-67);

Retrieving at least one player key from a nonvolatile memory (Column 9; lines 35-58; and Column 11, lines 18-30);

Using the at least one player key with a broadcast encryption system (Column 12, lines 35-67);

Using the result of the broadcast encryption system to decrypt at least a portion of the audiovisual content (Column 12, lines 35-67; and Column 14, lines 1-63);

But does not explicitly disclose selecting a variant from a plurality of variants for each of a plurality of portions of the audiovisual content, where: the player is capable of decrypting the selected variants, and the player lacks at least one cryptographic key required to decrypt at least one non-selected variant for each portion; decrypting each selected variant; reading program logic for a Turing-complete interpreted language from the medium; and using an interpreter to execute the program logic, where the interpreter performs operations specified in the program logic to respond to selections from a user.

Benaloh, however, discloses selecting a variant from a plurality of variants for each of a plurality of portions of the audiovisual content, where: the player is capable of decrypting the selected variants, and the player lacks at least one cryptographic key required to decrypt at least one non-selected variant for each portion; and decrypting each selected variant (Column 9, line 61 to Column 11, line 12). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the digital content protection scheme of Benaloh into the information recording/reproducing system of Asano in order to allow the system to detect pirated copies of content and trace it back to the specific player used to pirate the content while providing all content players with identical data on the storage medium.

Kyle, however, discloses reading program logic for a Turing-complete interpreted language from the medium; and using an interpreter to execute the program logic, where the interpreter performs operations specified in the program logic to respond to selections from a user (Column 3, line 28 to Column 4, line 30; Column 4, line 57 to Column 5, line 14; and Column 7, line 59 to Column 8, line 5). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the self protecting data package system of Kyle into the information recording/reproducing system of Asano as modified by Benaloh in order to allow the system to update the player and anti-virus

software, thereby maintaining security of the system with ease, as well as to provide self-sufficient data packages that can perform compression, decryption, virus checking, etc. without the need of specialized hardware or software.

5. Claim 14 is rejected under 35 U.S.C. 103(a) as being unpatentable over Asano in view of Benaloh, further in view of Lumelsky (U.S. Patent 6,529,950).

Asano as modified by Benaloh does not explicitly disclose means for reducing the output quality of the audiovisual content if a security requirement specified by the medium for high-quality output is not met.

Lumelsky, however, discloses means for reducing the output quality of the audiovisual content if a security requirement specified by the medium for high-quality output is not met (Column 4, lines 23-31; and Column 10, line 58 to Column 11, line 6). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the content quality levels of Lumelsky into the information recording/reproducing system of Asano as modified by Benaloh in order to allow players of varying capabilities to render the content in a quality level that can be played efficiently by each player, and/or to allow the user to choose whether to view higher or lower quality content.

6. Claim 17 is rejected under 35 U.S.C. 103(a) as being unpatentable over Asano in view of Benaloh and Kyle, further in view of Foote (U.S. Patent 6,164,853).

Asano as modified by Benaloh and Kyle may not disclose that the user selections include button presses on a remote control.

Foote, however, discloses that the user selections include button presses on a remote control (Column 1, lines 25-39). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the remote of Foote into the information recording/reproducing system of Asano as modified by Benaloh and Kyle in order to enable a user to operate the player from the comfort of the user's chair or sofa, thereby eliminating the need to physically interact with the player itself.

7. Claim 18 is rejected under 35 U.S.C. 103(a) as being unpatentable over Asano in view of Benaloh and Kyle, further in view of Ford (Ford, Susan, "Advanced Encryption Standard (AES) Questions and Answers", 10/2/2000, pp. 1-5, obtained from http://www.nist.gov/public_affairs/releases/aesq&a.htm).

Asano as modified by Benaloh and Kyle discloses the method of claim 16, in addition, Kyle discloses that the program logic directs the player to perform a cipher operation via an interpreter (Column 3, line 28 to Column 4, line 30; Column 4, line 57 to Column 5, line 14; and Column 7, line 59 to Column 8, line 5); but does not disclose that the cipher operation is an AES cipher operation.

Ford, however, discloses that the cipher operation is an AES block cipher operation (Pages 1-5). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the encryption algorithm of

Ford into the information recording/reproducing system of Asano as modified by Benaloh and Kyle in order to use an encryption algorithm that provides high security, performance, efficiency, ease of implementation, and flexibility and that is easy to defend against power and timing attacks.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeffrey D. Popham whose telephone number is (571)-272-7215. The examiner can normally be reached on M-F 9:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571)272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Jeffrey D Popham
Examiner
Art Unit 2137

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER